

McAfee Firewall Enterprise 8.3.2P04

Contents

- ▶ [About this release](#)
- ▶ [Resolved issues](#)
- ▶ [Installation instructions](#)
- ▶ [Known issues](#)
- ▶ [Find product documentation](#)

About this release

This document contains important information about the current release. We strongly recommend that you read the entire document.

McAfee® Firewall Enterprise (Firewall Enterprise) version 8.3.2P04 resolves issues present in the previous release.

Supported firewall types

Firewall Enterprise supports these firewall types.

- McAfee® Firewall Enterprise appliances
- McAfee® Firewall Enterprise, Virtual Appliance
- McAfee® Firewall Enterprise on Crossbeam X-Series Platforms

These features are not supported on Crossbeam X-Series Platforms for this release:

- Firewall Enterprise Admin Console



Use a McAfee® Firewall Enterprise Control Center (Control Center) Management Server to manage Firewall Enterprise on Crossbeam X-Series Platforms.

- Multicast dynamic routing using the PIM-SM protocol
- Hybrid mode (configuring standard and transparent mode on the same firewall)
- Default route failover
- Quality of Service (QoS)
- Transparent (bridged) mode for these configurations:
 - Dual-Box High Availability (DBHA)
 - Multi-application serialization

- DBHA active-active mode



Active-standby DBHA is supported.

- Crossbeam X-Series Operating System (XOS) features:
 - Virtual Application Processor (VAP) group hide-vlan-header parameter
 - Equal-cost multi-path routing
 - Configuration of the VRRP MAC address



If you need functionality similar to the VRRP MAC address, Crossbeam recommends configuring a user-defined MAC address on each traffic circuit/interface pair included in the VRRP failover group. See the Crossbeam support knowledge base article 0004069.

Compatible McAfee products

Firewall Enterprise is compatible with the following McAfee products.

- McAfee® Firewall Enterprise ePolicy Orchestrator® Extension
- McAfee® Firewall Enterprise Control Center
- McAfee® Logon Collector
- McAfee® Endpoint Intelligence Agent (McAfee EIA)
- McAfee® Event Reporter

For more information, see:

- **McAfee firewall products and versions that Firewall Enterprise supports** — KnowledgeBase article [KB67462](#)
- **Firewall products and interoperability with Firewall Enterprise** — Technical Note: *Using McAfee Firewall Enterprise with Other McAfee Products*

Requirements

Before you install this version, make sure the Admin Console and Firewall Enterprise requirements are met.

Admin Console requirements

The computer that hosts the Admin Console must meet these requirements.


Table 1-1 Admin Console minimum requirements

Component	Requirements
Operating system	One of these Microsoft operating systems: <ul style="list-style-type: none">• Windows Server 2008• Windows 7• Windows 8 Compatible legacy Microsoft operating systems: <ul style="list-style-type: none">• Windows XP Professional• Windows Vista
Web browser	One of the following: <ul style="list-style-type: none">• Microsoft Internet Explorer, version 6 or later• Mozilla Firefox, version 1.0 or later
Hardware	<ul style="list-style-type: none">• 2 GHz x86-compatible processor• 2 GB of memory• 300 MB of available disk space• CD drive• 1024 x 768 display• Network card (to connect to your firewall)• USB port

Firewall Enterprise requirements

The firewall must meet these requirements.

Table 1-2 Minimum requirements by Firewall Enterprise type

Firewall type	Platform requirements
Firewall Enterprise appliance	<p>Appliance with a valid support contract:</p> <ul style="list-style-type: none"> • 1 GB of memory • AMD64-compatible processor
Firewall Enterprise, Virtual Appliance	<p>Virtualization server:</p> <ul style="list-style-type: none"> • Hypervisor operating system — VMware ESX/ESXi version 4.0 or later <div>  <p>Firewall Enterprise, Virtual Appliance is installed in 64-bit mode by default. Your system must support Intel VT technology (or equivalent) to run properly in a virtual environment. Before starting the virtual appliance, verify that VT is enabled in your computer BIOS.</p> </div> <ul style="list-style-type: none"> • Hardware resources: <ul style="list-style-type: none"> • 2 virtual processors • AMD64-compatible processor • 1 GB of memory • 30 GB of free disk space • 2 or more NICs of type e1000 • Internet connectivity — The firewall requires a persistent Internet connection to maintain an active license and full functionality.
Firewall Enterprise on Crossbeam X-Series Platforms	<p>Crossbeam X-Series Platform:</p> <ul style="list-style-type: none"> • Chassis — X50, X60, or X80-S • XOS version — 9.6.5 and later, 9.7.1 and later, 9.9.x, or 10.0 • Application Processor Module — APM-50 or APM-9600 <ul style="list-style-type: none"> • At least one local disk (RAID 0 and RAID 1 disk configurations are supported; two-disk, non-RAID configurations are not supported) • 12 GB of memory (minimum) • Network Processor Module — NPM-50, NPM-86x0, or NPM-96x0 • CBI package — MFE-8.3.2-9.mr1.cbi

McAfee EIA requirements

Systems must meet these requirements to install McAfee® Endpoint Intelligence Agent (McAfee EIA).

Table 1-3 McAfee EIA minimum requirements

Component	Requirements
Operating system	One of these 32-bit or 64-bit Microsoft operating systems: <ul style="list-style-type: none">• Windows XP Service Pack 2 and later• Windows 2012• Windows 2012 R2• Windows 8.1• Windows 7• Windows Server 2003 Service Pack 1 and later• Windows Server 2003 R2 Service Pack 1 and later• Windows Server 2008• Windows Server 2008 R2
Hardware	<ul style="list-style-type: none">• 2 GHz x86-compatible processor• 2 GB of memory• 300 MB of available disk space• 1024 x 768 display• Network card (to connect to your firewall)• One of the following:<ul style="list-style-type: none">• USB port• CD drive
Other McAfee products	McAfee EIA deployment requires: <ul style="list-style-type: none">• McAfee® Endpoint Intelligence Manager (McAfee EIM) version 2.2.0• ePolicy Orchestrator version 4.6.5, 5.x, and later• McAfee Agent version 4.8.0 patch 2 and later

Resolved issues

These issues are resolved in this release of the product. For a list of issues fixed in earlier releases, see the Release Notes for the specific release.

Admin Console

Improves the performance of the Admin Console dashboard when there are many IPFilter sessions (978884)

Certificate management

- Updates Trusted Internet CA certificates from Mozilla.org (968798, 982670)
- Supports FIPS 186-4 RSA key generation (982188)

Kernel

- Allows the source port NAT to work with the localhost address (965990)
- Provides additional integrity checks for the IPFilter session list (964397)
- Resolves IPsec code locking (923168 and 979940)

- Improves memory in IPFilter (972730)
- Prevents duplicate IPFilter sessions from accumulating (947870)
- Improves scanning for IPS data processing (961542)
- Resolves an issue with the use of dynamic hosts in network address translation (NAT) and redirect network objects attached to IPFilter policy rules (974524)

Policy

Improves compiler performance for policies with many IP address endpoints (957088)

Proxy

H.323 — Modifies the H.323 proxy to allow more audio and video codecs when enforcement is off (959014)

SNMP

- Prevents the SNMP proxy from creating excessive load sharing exceptions (947870)
- Allows an agent or proxy to bind in the same zone consistently (969902)

TrustedSource

Improves the auto-reconnect of ACLD to McAfee® Global Threat Intelligence™ (McAfee GTI) servers (959479)

Common Vulnerabilities and Exposures (CVEs)

File — Includes a fix for CVE-2012-1571, CVE-2013-7345, CVE-2014-1943, CVE-2014-2270, FreeBSD-SA-14:16.file; see [KB82324](#) for more information (977934)

Kernel

- Includes maintenance updates; see [KB81838](#) for more information. Firewall Enterprise is not vulnerable to CVE-2014-3000 (965043)
- Imports a fix for CVE-2014-3880, FreeBSD-EN-14:06.exec; see [KB82324](#) for more information (978290)
- Imports a fix for CVE-2014-3952, FreeBSD-SA-14:17.kmem; See [KB82324](#) for more information (981441)

OpenSSL

Addresses these CVEs and includes updates:

- CVE-2014-0224, CVE-2014-0221, CVE-2014-0195, and CVE-2014-3470; see [KB82150](#) for more information (973042)
- Includes maintenance updates, see [KB81858](#) for more information; Firewall Enterprise is not vulnerable to CVE-2014-0198 (966337)

Proxies — Provides additional protections for CVE-2014-0160 (Heartbleed) (969677)

- Blocks Heartbleed when proxy content inspection is disabled
- Adds auditing to the HTTP proxy when a Heartbleed attack is detected — both when SSL content inspection is enabled and disabled

Sendmail — Includes a fix for CVE-2014-3956, FreeBSD-SA-14:11.sendmail; see [KB82324](#) for more information (978297)

Installation instructions

To bring your firewall to version 8.3.2P04, follow the patch installation process appropriate for your environment.

Before you begin

The firewall must be at version 8.3.2P03.

- **Standalone or HA cluster** — See the *McAfee Firewall Enterprise Product Guide*, version 8.3.2P03.
- **Control Center-managed firewall or HA cluster** — See the *McAfee Firewall Enterprise Control Center Release Notes*, version 5.3.2P02 and *McAfee Firewall Enterprise Control Center Product Guide*, version 5.3.2.



If your firewall is managed by Control Center, it must be at version 5.3.2P02 or later to manage firewalls at version 8.3.2P03.

- **Crossbeam X-Series Platforms firewall** — See the *McAfee Firewall Enterprise on Crossbeam X-Series Platforms Installation Guide*, version 8.3.x.

Known issues

For a list of known issues in this product release, see this McAfee KnowledgeBase article: [KB79061](#).

Find product documentation

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

Task

- 1 Go to the McAfee ServicePortal at <http://support.mcafee.com> and click **Knowledge Center**.
- 2 Enter a product name, select a version, then click **Search** to display a list of documents.

Product documentation

Every McAfee product has a comprehensive set of documentation.

McAfee Firewall Enterprise documentation includes:

Typical documents

- *McAfee Firewall Enterprise Product Guide*
- *McAfee Firewall Enterprise Release Notes*
- *McAfee Firewall Enterprise ePolicy Orchestrator Extension Integration Guide*
- *McAfee Firewall Enterprise Command Line Interface Reference Guide*

- Technical Note — *Using McAfee Firewall Enterprise with Other McAfee products*
- Application Note — *Configuring Department of Defense Common Access Card Authentication on McAfee Firewall Enterprise*

Hardware

- *McAfee Firewall Enterprise on Crossbeam X-Series Platforms Installation Guide*
- *McAfee Firewall Enterprise, Virtual Appliance Installation Guide*
- *McAfee Firewall Enterprise, Virtual Appliance Evaluation for Desktop Installation Guide*
- *McAfee Firewall Enterprise Quick Start Guide*
- *McAfee Firewall Enterprise Hardware Guide, models S4016, S5032, S6032, and S7032*
- *McAfee Firewall Enterprise Hardware Guide, models S1104, S2008, and S3008*

Certification

- *McAfee Firewall Enterprise Common Criteria Evaluated Configuration Guide*
- *McAfee Firewall Enterprise FIPS 140-2 Configuration Guide*
- *McAfee Firewall Enterprise FIPS 140-2 Level 2 Kit Installation Guide, S Models*

Copyright © 2014 McAfee, Inc. Do not copy without permission.

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.